UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/591,927	06/12/2000	Junichi Miura	16869P-008100	3690

20350 7590 01/15/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
QUINONES, EDEL H	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/15/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/591,927	MIURA ET AL.	
	Examiner	Art Unit	
	Edel H Quinones	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

III. Detailed Action

1. Claims 1-34 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement filed on 7/16/2001 complies with the provisions of MPEP § 609. It has been placed in the application file, and the information referred to therein has been considered as to the merits.

Claim Objections

3. Claim 25 is objected to because of the following informalities:

Claim 25, line 6, "encrypt data on inputted" should read, "encrypt data inputted"

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-2, 5-6, 8-9, 11-12, 14, 16-17, 19, 21-24, 26, 28-30, 32 and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Reiche (U.S. Patent 6,092,196).

In regards to claim 1, Reiche teaches an electronic authentication method (col. 1, lines 26-28) comprising: generating an identifier for contents (i.e. transaction ID) in a first information processing apparatus (i.e. customer server) (col. 4, line 50-65);

storing said identifier in a storage unit (i.e. database) (col. 5 , line 1);

transmitting said contents and said identifier to a second information processing apparatus (i.e. browser) (col. 5 , lines 2-6);

inputting data for said contents in said second information processing apparatus; transmitting said input data and said identifier from said second information apparatus to said first information apparatus (col. 5, lines 12-15);

and authenticating legitimacy of said input data (col. 5, lines 48-61) and invalidating said stored identifier (i.e. constructing a new transaction ID) if said received identifier matches said identifier in said storage unit in said first information processing apparatus (col. 6, lines 3-10).

In regards to claim 2, Reiche teaches wherein in said first information processing apparatus, said identifier is embedded (i.e. appended) in said contents prior to transmission of said contents to said second information processing apparatus (col. 5, lines 6-11).

In regards to claim 5, Reiche teaches an information processing method (i.e. user access control protocol) (col. 4, lines 20-21) comprising:

generating an identifier for contents (i.e. transaction ID) (col. 4, line 64);

storing said identifier (col. 5, line 1);

transmitting said contents and said identifier to an external apparatus (i.e. browser) (col. 5, lines 2-5);

receiving data from said external apparatus (col. 5, lines 43-55);

acquiring an identifier for said contents (col. 5, lines 56-58); and

carrying out processing based on said received data (col. 6, lines 3-7) and invalidating said stored identifier if said acquired identifier matches said stored identifier (i.e. constructing a new transaction ID) (col. 6, lines 8-10).

In regards to claim 6, Reiche teaches wherein said identifier is embedded (i.e. appended) in said contents prior to transmission of said contents to said external apparatus (col. 5, lines 6-11).

In regards to claim 8, Reiche teaches an electronic authentication system (i.e. an authentication server for use in a data network) (col. 4, lines 14-15) comprising a first information processing apparatus (i.e. customer server) (col. 4, line 57) and a second information processing apparatus (i.e. browser) (col. 4, line 56) wherein:

said first information processing apparatus comprises: a means for generating an identifier for contents (i.e. transaction ID) (col. 4, line 64);

a storage means (i.e. database) for storing said identifier (col. 5, line 1); and

a means (i.e. URL) for transmitting said contents and said identifier to said second information processing apparatus (col. 5, lines 6-8);

said second information processing apparatus comprises: a means for inputting data for said received contents (i.e. an input device such as a keyboard or mouse inherent to a web browser client machine such as the ones depicted in Figure 1); and

a means for transmitting said input data and said identifier to said first information processing apparatus (i.e. digital network) (Figure 1, element 160); and

there is further provided a processing means for authenticating legitimacy of said input data received by said first information processing apparatus (i.e. comparing the transaction ID to the transaction ID held in memory) (col. 5, lines 57-58) and invalidating said stored identifier (i.e. the customer server then construct a new transaction ID that is locally stored and it is also embedded in a cookie) (col. 6, lines 8-10) if said identifier received by said first information processing apparatus matches said identifier stored in said storage means (col. 6, lines 3-5).

In regards to claim 9, Reiche teaches wherein said first information processing apparatus further includes an embedding means (i.e. URL) for embedding said identifier in said contents (col. 5, lines 6-9); and said first information processing apparatus transmits said contents including said embedded identifier to said second information processing apparatus (col. 5, lines 1-4).

In regards to claim 11, Reiche teaches an information processing apparatus (i.e. customer server) (figure 1, element 120) comprising:

a generation means (i.e. authentication deamon) for generating an identifier for contents (col. 8, line 65);

a storage means (i.e. memory table) (figure 1, element 122) for storing said identifier;

a transmission means (i.e. digital network) (col. 8, line 6) for transmitting said contents and said identifier to an external apparatus (i.e. web browser/client) (figure 1, elements 100-108);

a reception means (i.e. http server) (figure 1, element 126) for receiving data from said external apparatus;

an acquirement means (i.e. authentication deamon) (col. 9, lines 59-63) for acquiring an identifier for said contents from said received data; and

a processing means for carrying out processing based on said received data (col. 9, lines 63-66) and invalidating said identifier stored in said storage means if said acquired identifier matches said stored identifier (col. 10, lines 11-21).

In regards to claim 12, Reiche teaches said apparatus further comprising an embedding means (i.e. URL) for embedding said identifier in said contents (col. 9, lines 1-3), wherein said transmission means transmits said contents including said embedded identifier to said external apparatus (col. 9, lines 6-11).

In regards to claim 14, Reiche teaches an information processing apparatus (i.e. web browser/client) (figure 1, element 100-108) comprising:

a contents requesting means (i.e. HTTP 1.X) (col. 8, lines 26-29) for requesting an external information processing apparatus to transmit contents;

a reception means (i.e. HTTP 1.X) (col. 8, lines 26-29) for receiving said requested contents and an identifier embedded in said contents;

an extraction means (i.e. AD CGI) for extracting (i.e. decoding) said identifier from said contents (col. 9, lines 45-49);

an input means (i.e. an input device such as a keyboard or mouse inherent to a web browser client machine such as the ones depicted in Figure 1) for inputting data for said contents;

and a transmission means (i.e. digital network) (figure 1, element 160) for transmitting said input data and said identifier to said external information processing apparatus.

In regards to claim 16, Reiche teaches a storage medium (i.e. customer server) (figure 1, element 120) for storing information readable by a computer, said medium characterized in that said information includes:

a generation function (i.e. authentication deamon) for generating an identifier for contents (col. 8, line 65);

a storage function (i.e. memory table) for storing said generated identifier (figure 1, element 122);

a transmission function (col. 5, lines 6-8) for transmitting said contents and said identifier to an external apparatus (col. 5, lines 6-8);

a reception function (i.e. HTTP 1.X) (col. 8, lines 26-29) for receiving data from said external apparatus;

an acquirement function (ie. AD CGI) for acquiring (i.e. decoding) an identifier for said contents from said received data (col. 9, lines 45-49); and

a processing function (i.e. Authentication Daemon on the Customer Server) for authenticating legitimacy of said received data (col. 9, lines 59-67) and invalidating said stored identifier (i.e. generating a new transaction ID) if said acquired identifier matches said stored identifier (col. 10, lines 18-21).

In regards to claim 17, Reiche teaches said medium characterized in that said information further has a function (i.e. URL) for embedding said identifier in said contents (col. 9, lines 1-3), wherein said transmission function transmits said contents including said embedded identifier to said external apparatus (col. 9, lines 6-11).

In regards to claim 19, Reiche teaches a storage medium (i.e. web browser/client) (figure 1, elements 100-108) for storing information readable by a computer, said medium characterized in that said information includes:

a contents requesting function (i.e. HTTP 1.X) (col. 8, lines 26-29) for requesting an external information processing apparatus (i.e. customer server) (figure 1, elements 120, 150) to transmit contents;

a reception function (i.e. HTTP 1.X) (col. 8, lines 26-29) for receiving said requested contents and an identifier (i.e. transaction ID) (col. 4, line 65) embedded in said contents;

an extraction function (i.e. AD CGI) for extracting (i.e. decoding) said identifier from said contents (col. 9, lines 45-49);

an input function (i.e. an input device such as a keyboard or mouse inherent to a web browser client machine such as the ones depicted in Figure 1) for inputting data for said contents; and

a transmission function (i.e. digital network) (figure 1, element 160) for transmitting said input data and said identifier to said external information processing apparatus.

In regards to claim 21, Reiche teaches an electronic authentication method (i.e. user access control protocol) (col. 4, lines 20-21) comprising:

generating an identifier (i.e. transaction ID) (col. 8, line 66) for contents in a first information processing apparatus (i.e. customer server) (col. 4, line 57);

driving said first information processing apparatus to store said identifier and the present time as a storage time in a storage unit (i.e. memory table) (col. 8, line 66-67 and col. 9, line 1)

(Note: the examiner presumes that storing the URL expiry time may also involve storing the present time)

transmitting said contents and said identifier to a second information processing apparatus (col. 9, line 5-8);

inputting data for said contents received by said second information processing apparatus in said second information processing apparatus (col. 9, line 28-30);

transmitting said input data and said identifier from said second information processing apparatus to said first information processing apparatus (col. 9, lines 38-39); and

invalidating said identifier stored in said storage unit if said identifier received by said first information processing apparatus is not stored in said storage unit or a time of a predetermined length has lapsed since said storage time stored in said storage unit (col. 9, lines 63-65).

In regards to claim 22, Reiche teaches an electronic authentication method (i.e. user access control protocol) (col. 4, lines 20-21), comprising:

generating an identifer (i.e. transaction ID) (col. 4, line 64) for an access to contents in a first information processing apparatus (i.e. customer server) (col. 4, line 57);

storing said identifier in a storage unit (i.e. database) (col. 5, line 1);

transmitting said contents and said identifier to a second information processing apparatus (i.e. browser) (col. 5, lines 2-6);

inputting data for said contents received by said second information processing apparatus in said second information processing apparatus (col. 9, lines 27-30);

transmitting said input data and said identifier from said second information processing apparatus to said first information processing apparatus (col. 9, lines 38-39); and

validating said input data only for this transaction if said identifier received by said first information processing apparatus matches said identifier stored in said storage unit (col. 9, line 63-67).

In regards to claim 23, Reiche teaches a storage medium (i.e. customer server) (figure 1, element 120) for storing information readable by a computer, said medium characterized in that said information includes:

a generation function (i.e. authentication daemon) for generating an identifier for contents (col. 8, line 65);

a storage function (i.e. authentication daemon) for storing said generated identifier in a storage means (i.e. memory table);

an acquirement function (i.e. AD CGI) for acquiring an identifier (i.e. transaction ID) for said contents from said data received from an external apparatus (col. 9, lines 45-49); and

a processing function (i.e. Authentication Daemon on the Customer Server) for carrying out processing based on said received data and invalidating (i.e. generating a new transaction ID) said identifier stored in said storage means if said acquired identifier matches said stored identifier (col. 10, lines 18-21).

In regards to claim 24, Reiche teaches an authentication method (i.e. user access control protocol) (col. 4, line 20) in a system in which a first computer (i.e. client) making a request for a service (col. 8, line 47) is connected to a second computer (i.e. secure customer HTTP server) rendering services via a network (col. 8, line 48), requested contents being transmitted from the

second computer to the first computer, data being transmitted from the first computer to the second computer associated with the contents, said method comprising:

generating at the second computer an access number (i.e. a 16 byte random transaction ID) (col. 8, line 66) for accessing the contents and cataloging the access number in a storage unit (i.e. memory table) (col. 8, line 67);

embedding the access number in the contents (col. 9, lines 1-3) so that the access number is invisible (col. 9, lines 12-14) and transmitting the contents to the first computer (col. 9, lines 6-9);

displaying the contents at the first computer (col. 9, lines 24-28);

adding the access number fetched from the contents to data inputted (col. 9, lines 28-45) associated with the contents and transmitting the inputted data to the second computer (col. 9, lines 51-56); and

authenticating validity at the second computer of the received data when the received access number has been cataloged (col. 9, lines 63-65) and invalidating the cataloged access number (col. 10, lines 17-19).

In regards to claim 26, Reiche teaches a storage medium for storing a program which can be read by a computer (i.e. customer server) (figure 1, element 120), wherein the program (i.e. authentication daemon) has a function of generating an access number (i.e. random transaction ID) for accessing contents requested from the outside (col. 8, line 65), a function of cataloging the generated access number (i.e. authentication daemon) in a storage unit (i.e. memory table) (col. 8, lines 66-67), a function of embedding the access number in the contents (col. 9, lines 1-3) so that the access number is invisible (col. 9, lines 12-14) and transmitting the contents to the

outside (col. 9, lines 6-9), a function of receiving data to which the access number is added from the outside (col. 9, lines 57-67), and a function of authenticating validity on the received data when the received access number has been cataloged (col. 9, lines 63-65) and invalidating the cataloged access number (col. 10, lines 17-19).

In regards to claim 28, Reiche teaches a storage medium for storing a program which can be read by a computer (i.e. web browser/client) (figure 1, elements 100-108), wherein the program has a function of displaying contents received from the outside (i.e. HTTP 1.X) (col. 8, lines 26-29), a function of receiving data input associated with the contents (i.e. HTTP 1.X) (col. 8, lines 26-29), a function of fetching an access number (i.e. transaction ID) (col. 4, line 65) embedded in the contents so that the access number is invisible (col. 9, lines 12-14), and a function of adding the access number to the inputted data (col. 9, lines 1-3) and transmitting the data to the outside (col. 9, lines 6-9).

In regards to claim 29, Reiche teaches a server apparatus comprising:

a processor (figure 1, element 120);

a storage device (figure 1, element 122);

a network interface (figure 1, element 160); and a bus interconnecting said processor, said storage device and said network interface (i.e. internal bus inherent to the server);

wherein said processor generates an identifier for contents (col. 8, line 65) and stores said identifier into said storage device (i.e. memory table) (col. 8, line 67); and wherein said processor transmits said contents and said identifier to an external apparatus via said network interface (col. 9, lines 6-9); and wherein said processor receives data from said external apparatus via said network interface (col. 9, lines 57-67); and thereupon acquires from said data

an identifier for said contents from said received data (col. 9, lines 45-49); and wherein said processor performs processing based on said received data (col. 9, lines 63-65) and invalidates said identifier stored in said storage means if said acquired identifier matches said stored identifier (col. 10, lines 17-19).

In regards to claim 30, Reiche teaches wherein in said apparatus, said processor further embeds said identifier in said contents (col. 9, lines 1-3); and wherein said processor transmits said contents including said embedded identifier to said external apparatus (col. 9, lines 6-9).

In regards to claim 32, Reiche teaches a client apparatus comprising:

a processor (figure 1, element 100);

an input device (i.e. an input device such as a keyboard or mouse inherent to a web browser client machine such as the ones depicted in Figure 1);

a network interface (figure 1, element 160); and a bus interconnecting said processor, said input device and said network interface (i.e. internal bus inherent to the server);

wherein said processor requests an external information processing apparatus to transmit contents via said network interface (col. 8, line 47); and wherein said processor receives said requested contents and an identifier embedded in said contents; and thereupon, said processor extracts said identifier from said contents (col. 9, lines 6-9); and wherein said processor receives input data for said contents from said input device (col. 9, lines 28-30); and wherein said processor transmits said input data and said identifier to said external information processing apparatus via said network interface (col. 9, lines 38-49).

In regards to claim 34, Reiche teaches an information processing apparatus (figure 1, element 100) comprising:

a means for acquiring a contents from an external information processing apparatus (figure 1, element 160);

a means for receiving the contents (i.e. HTTP 1.X) (col. 8, lines 26-29);

a means for inputting a data with respect to the contents (i.e. an input device such as a keyboard or mouse inherent to a web browser client machine such as the ones depicted in Figure 1);

a means for sending the inputted data and an identifier of the contents to the external information processing apparatus (i.e. HTTP 1.X) (col. 8, lines 26-29); and

a means for displaying that an access is impossible if the contents is accessed at least once (i.e. an output device such as a monitor inherent to a web browser client machine such as the ones depicted in Figure 1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3-4, 7, 10, 13, 15, 18, 20, 25, 27, 31 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reiche (U.S. Patent 6,092,196) in view of Curry et al. (U.S. Patent 6,237,095 and Curry hereinafter).

The teachings of Reiche have been discussed above.

In regards to claims 3, Reiche does not teach further comprising: embedding an encryption key in said contents in said first information processing apparatus prior to transmission of said contents to said second information processing apparatus; encrypting said input data in said second processing apparatus by using said encryption key prior to transmission of said input data to said first information processing apparatus; and decrypting said received input data in said first information processing apparatus.

Curry teaches embedding an encryption key in said contents in said first information processing apparatus prior to transmission of said contents to said second information processing apparatus (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); encrypting said input data in said second processing apparatus by using said encryption key prior to transmission of said input data to said first information processing apparatus (col. 5, lines 31-41); and decrypting said received input data in said first information processing apparatus (col. 5, lines 42-44).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include further comprising: embedding an encryption key in said contents in said first information processing apparatus prior to transmission of said contents to said second information processing apparatus; encrypting said input data in said second processing apparatus by using said encryption key prior to transmission of said input data to said first information processing apparatus; and decrypting said received input data in said first information processing apparatus with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 4, Reiche does not teach wherein: said embedded encryption key is a public key; said received input data is decrypted using a private key associated with said public key; and said public key and said private key are generated in said first information processing apparatus.

Curry teaches wherein: said embedded encryption key is a public key (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); said received input data is decrypted using a private key associated with said public key (i.e. the recipient's computer contains the corresponding private key) (col. 5, lines 42-43); and said public key and said private key are generated in said first information processing apparatus (i.e. to use P.G.P., a user generates a complete RSA key set containing both a public and a private component) (col. 5, lines 24-26).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein: said embedded encryption key is a public key; said received input data is decrypted using a private key associated with said public key; and said public key and said private key are generated in said first information processing apparatus with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 7, Reiche does not teach further comprising: embedding an encryption key in said contents prior to transmission of said contents to said external apparatus; and receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier.

Curry teaches further comprising: embedding an encryption key in said contents prior to transmission of said contents to said external apparatus (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); and receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier (i.e. the recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include further comprising: embedding an encryption key in said contents prior to transmission of said contents to said external apparatus; and receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 10, Reicher teaches claim 9 as discussed above.

Reicher, however, does not teach wherein said first information processing apparatus transmits said contents, said contents further including an embedded encryption key, to said second information processing apparatus; and said first information processing apparatus further comprises a reception means for receiving an identifier encrypted by using said encryption key and decrypting said encrypted identifier.

Curry teaches wherein said first information processing apparatus transmits said contents, said contents further including an embedded encryption key, to said second information

processing apparatus (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); and said first information processing apparatus further comprises a reception means (i.e. email) (col. 5, line 36) for receiving an identifier encrypted by using said encryption key (i.e. the message is encrypted with IDEA and the IDEA key is encrypted with the intended recipient's public key) (col. 5, lines 39-41) and decrypting said encrypted identifier (i.e. the recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein said first information processing apparatus transmits said contents, said contents further including an embedded encryption key, to said second information processing apparatus; and said first information processing apparatus further comprises a reception means for receiving an identifier encrypted by using said encryption key and decrypting said encrypted identifier with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 13, Reiche teaches claim 12 as discussed above.

Reiche, however, does not teach wherein said transmission means transmits said contents further including said embedded encryption key to said external apparatus; and there is further provided a reception means for receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier.

Curry teaches wherein said transmission means transmits said contents further including said embedded encryption key to said external apparatus (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); and there is further provided a reception means for receiving an identifier encrypted by using said encryption key (i.e. the message is encrypted with IDEA and the IDEA key is encrypted with the intended recipient's public key) (col. 5, lines 39-41) and decrypting said received encrypted identifier (i.e. the recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein said transmission means transmits said contents further including said embedded encryption key to said external apparatus; and there is further provided a reception means for receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 15, Reiche teaches the apparatus of claim 14 as discussed above.

Reiche, however, does not teach said apparatus further comprising an encryption means for encrypting said input data by using an encryption key additionally embedded in said contents received by said reception means.

Curry teaches said apparatus further comprising an encryption means for encrypting said input data by using an encryption key (i.e. the message is encrypted with IDEA and the IDEA

key is encrypted with the intended recipient's public key) (col. 5, lines 39-41) additionally embedded in said contents received by said reception means (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include said apparatus further comprising an encryption means for encrypting said input data by using an encryption key additionally embedded in said contents received by said reception means with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 18, Reiche teaches the storage medium of claim 17 as discussed above.

Reiche, however, does not teach said medium characterized in that: said transmission function transmits said contents further including said embedded encryption key to said external apparatus; and said information further includes a function for receiving said data encrypted by using said encryption key and decrypting said received encrypted data.

Curry teaches said medium characterized in that: said transmission function transmits said contents further including said embedded encryption key to said external apparatus (i.e. [making the] public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); and said information further includes a function for receiving said data encrypted by using said encryption key (i.e. the user can receive secure e-mail only at his own computer) (col. 5, lines 5-6) and decrypting said received encrypted data (i.e. the

recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include said medium characterized in that: said transmission function transmits said contents further including said embedded encryption key to said external apparatus; and said information further includes a function for receiving said data encrypted by using said encryption key and decrypting said received encrypted data with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 20, Reiche teaches the storage medium of claim 19 as discussed above.

Reiche, however, does not teach said medium characterized in that said information further includes a function for encrypting said input data by using an encryption key additionally embedded in said contents received by said reception function.

Curry teaches said medium characterized in that said information further includes a function for encrypting said input data (col. 5, lines 34-48) by using an encryption key (i.e. public key) (col. 5, line 26) additionally embedded in said contents (i.e. email) (col. 5, lines 27-28) received by said reception function.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include said medium characterized in that said information further includes a function for encrypting said input data by using an encryption key additionally embedded in said contents received by said

reception function with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 25, Reiche teaches the method of claim 24.

Reiche, however, does not teach wherein the second computer generates a public key and a private key for accessing the contents and catalogs the public key and the private key in the storage unit, embeds the public key in the contents so that the public key is invisible and transmits the contents to the first computer, allows the first computer to encrypt data on inputted associated with the contents by the public key fetched from the contents and transmit the data to the second computer, and decrypt the received data by the public key cataloged when the received access number has been cataloged.

Curry teaches wherein the second computer generates a public key and a private key for accessing the contents and catalogs the public key and the private key in the storage unit (i.e. a user generates a complete RSA key set containing both a public and a private component) (col.5, lines 25-26), embeds the public key in the contents so that the public key is invisible and transmits the contents to the first computer (i.e. makes his public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28), allows the first computer to encrypt data on inputted associated with the contents by the public key fetched from the contents and transmit the data to the second computer (i.e. encrypt the IDEA key itself using the public key provided by the intended recipient) (col. 5, lines 34-36), and decrypt the received data by the public key cataloged when the received access number has been cataloged (i.e. the recipients computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein the second computer generates a public key and a private key for accessing the contents and catalogs the public key and the private key in the storage unit, embeds the public key in the contents so that the public key is invisible and transmits the contents to the first computer, allows the first computer to encrypt data on inputted associated with the contents by the public key fetched from the contents and transmit the data to the second computer, and decrypt the received data by the public key cataloged when the received access number has been cataloged with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 27, Reiche teaches the storage medium of claim 26 as discussed above.

Reiche, however, does not teach wherein the program has a function of generating a public key and a private key for accessing the contents, a function of cataloging the public key and the private key in the storage unit, a function of embedding the public key and the private key in the contents so that the public key is invisible and transmits the contents to the outside, a function of receiving data encrypted by the public key from the outside, and a function of decrypting the received data by the public key cataloged when the received access number has been cataloged.

Curry teaches wherein the program has a function of generating a public key and a private key for accessing the contents (i.e. a user generates a complete RSA key set containing both a public and a private component) (col.5, lines 25-26), a function of cataloging the public

key and the private key in the storage unit (i.e. he stores his private key on his own personal computer) (col. 5, lines 29-30) (Note: the examiner presumes that the public key may also be stored), a function of embedding the public key and the private key in the contents so that the public key is invisible and transmits the contents to the outside (i.e. makes his public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28) (Note: the examiner presumes that the private key may also be embedded), a function of receiving data encrypted by the public key from the outside (i.e. the user can receive secure e-mail) (col. 5, lines 51-52), and a function of decrypting the received data by the public key cataloged when the received access number has been cataloged (i.e. the recipients computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein the program has a function of generating a public key and a private key for accessing the contents, a function of cataloging the public key and the private key in the storage unit, a function of embedding the public key and the private key in the contents so that the public key is invisible and transmits the contents to the outside, a function of receiving data encrypted by the public key from the outside, and a function of decrypting the received data by the public key cataloged when the received access number has been cataloged with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 31, Reiche teaches the apparatus of claim 30.

Reiche, however, does not teach wherein in said apparatus, said processor further transmits said contents, said contents further including said embedded encryption key, to said external apparatus; and wherein said apparatus receives an identifier encrypted using said encryption key; and thereupon decrypts said received encrypted identifier.

Curry teaches wherein in said apparatus, said processor further transmits said contents, said contents further including said embedded encryption key, to said external apparatus (i.e. makes his public key widely available by putting it in the signature block of all his e-mail messages) (col. 5, lines 26-28); and wherein said apparatus receives an identifier encrypted using said encryption key (i.e. the user can receive secure e-mail) (col. 5, lines 51-52); and thereupon decrypts said received encrypted identifier (i.e. the recipients computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message) (col. 5, lines 41-43).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein in said apparatus, said processor further transmits said contents, said contents further including said embedded encryption key, to said external apparatus; and wherein said apparatus receives an identifier encrypted using said encryption key; and thereupon decrypts said received encrypted identifier with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

In regards to claim 33, Reiche teaches the apparatus of claim 32.

Reiche, however, does not teach wherein in said apparatus, said processor further encrypts said input data using an encryption key additionally embedded in said contents received via said network interface.

Curry teaches wherein in said apparatus, said processor further encrypts said input data using an encryption key additionally embedded in said contents received via said network interface (i.e. encrypt the IDEA key itself using the public key provided by the intended recipient) (col. 5, lines 34-36).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Reiche with the teachings of Curry to include wherein in said apparatus, said processor further encrypts said input data using an encryption key additionally embedded in said contents received via said network interface with the motivation of providing security from those who might try to read the user's email (i.e. messages) remotely (Curry, col. 5, lines 44-45).

Other Prior Art Made of Record

6. A. Mi et al. (US Patent No. 6,418,472) discloses a system and method for using internet based caller id for controlling access to an object stored in a computer;

B. Atkinson et al. (US Patent No. 6,367,012) discloses embedding certifications in executable files for network transmission; and

C. Spagna et al. (US Patent No. 6,587,837) discloses a method for delivering electronic content from an online store.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Points of Contact

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H Quinones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheik can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quinones
Patent Examiner
Technology Center 2100

December 31, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100